AMENDMENTS TO THE SPECIFICATION

Please replace paragraph [0093] with the following amended paragraph:

[0093] The ~~rational~~ rationale behind this third example is that the work of signing a message in the presented signature scheme is governed by updating the secret key. Thus one could calculate how many ~~signature~~ signatures one can possibly issue during a time period given the computational power one has and then set s to this number. Then, one would constantly perform the secret key update, even if no message was signed. This approach would not change the response behavior of the system very much, but does not use a public archive and the signatures are smaller than in the first example.